April 25, 2022

Kevin Stine
Chief Cybersecurity Advisor and Chief, Applied Cybersecurity Division
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Via e-mail to CSF-SCRM-RFI@nist.gov

Mr. Stine,

BSA | The Software Alliance[1] appreciates the opportunity to provide the below responses to the National Institute of Standards and Technology's (NIST) request for information (Docket Number: 220210–0045). BSA appreciates NIST's open and transparent processes and commitment to engaging with industry.

BSA is the leading advocate for the global enterprise software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, providing the products and services that power governments and businesses. BSA members are also leaders in cybersecurity, having pioneered many of the software security best practices used throughout the industry today, including The BSA Framework for Secure Software, to which the NIST Secure Software Development Framework maps.

Since its development pursuant to Executive Order 13636, the NIST Cybersecurity Framework has provided a foundation for organizations' internal and external communications about cybersecurity risk management. As NIST considers whether and how to update the Framework, BSA urges NIST to do everything in its power to do ensure that the Cybersecurity Framework remains the host helpful 21 pages in cybersecurity. Too

[1] BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

often documents increase in volume but decline in value. One important source of value the Cybersecurity Framework provides is only including the cybersecurity information that NIST and its stakeholders identify as the most important. It would be detrimental to the value of the Framework, and consequently to the cybersecurity ecosystem, if the Framework were to grow beyond its current length. BSA understands that limiting the length of the document creates a significant challenge – but it is precisely NIST's ability to meet that challenge, to include only the most important concepts, language, and references, that create value.

Turning to the specific questions NIST asked in its RFI, BSA provides the following specific responses.

2. Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (e.g., supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?

Four drivers of the benefit the Framework creates stand out. First, because it is risk-based and flexible, it can be used by diverse organizations in any sector. Second, because it is widely used, it contains a lingua franca for communicating about cybersecurity risk management. Third, because it is written at an appropriate level, high enough to be universal but detailed enough to drive cybersecurity risk management, it is usable. Fourth, because organizations use it and provide their documents to NIST, the informative references lower the barrier while simultaneously amplifying the benefits to use.

With regards to NIST's specific question about cybersecurity metrics, BSA understands that measuring something as complex as cybersecurity is difficult but notes the inclusion of "Measuring Cybersecurity" in the NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1 April 25, 2019,[2] and strongly supports increased investment in "Research to understand challenges, insights, and gaps in cybersecurity measurement."

6. Additional ways in which NIST could improve the Cybersecurity Framework, or make it more useful.

While the Framework existing as a static document has benefits, for example, it is easy to share, NIST should consider whether it could increase the value of the Framework by rethinking its overall format. Similar to NIST evolving 800-53 from a static document, NIST

[2] NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1, April 2019, available at https://www.nist.gov/system/files/documents/2019/04/25/csf-roadmap-1.1-final-042519.pdf.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

should consider using software to build a navigable NIST Cybersecurity Framework Ecosystem that could also link and show the relationship between the Cybersecurity Framework, the Risk Management Framework, and the Privacy Framework, as well as mappings, links, informative references, etc.

Substantively, BSA notes three opportunities to make the Framework more useful. First, the Cybersecurity Framework and the Risk Management Framework should be mapped or reconciled to clearly show the relationship between the documents.

Second, NIST should discuss further the broader DevSecOps ecosystem, including how enterprises should consider software factories. As DoD notes, "A software supply chain 'has a' software factory, but the software factory itself is not an entire software supply chain."[3]

Third, further explanation of how threat and vulnerability assessments plug into the Framework, as well as additional informative references for effective threat and vulnerability assessments would improve the Framework. While information sharing should remain voluntary (based on an organization's cost-benefit analysis of legal, cybersecurity, and other tradeoffs), further discussion on the benefits of sharing information might incline more organizations to share information, and consequently improve the cybersecurity ecosystem as a whole. The Framework is a tool to help an organization understand its cybersecurity risk, i.e. the product of threats, vulnerabilities, and impacts. Further information on how organizations can use the Framework to manage these risks would be valuable. To be clear, NIST should not develop further threat or vulnerability assessment tools or guidance, but point to existing, high-quality assessments and explain how an organization can integrate these existing, high-quality assessments into their use of the Framework.

10. References that should be considered for inclusion within NIST's Online Informative References Program.

The Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,[4] directs each agency to "use the Framework for Improving Critical Infrastructure Cybersecurity, developed by the National Institute of Standards and Technology, to manage the agency's cybersecurity risk." Given this direction, NIST should share what it means for an agency to "use" the framework and agencies should provide to

[3] DoD Enterprise DevSecOps Strategy Guide, March 2021, available at https://dodcio.defense.gov/Portals/0/Documents/Library/DoDEnterpriseDevSecOpsStrategyGuide.pdf.

[4] Executive Order on Strengthening Federal Networks and Critical Infrastructure, May 11, 2017, available at https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

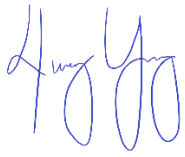
NIST, and NIST should make available, the cybersecurity risk documents created and used by agencies to comply with this requirement. With the obvious exception of information that is classified or otherwise needs to remain confidential, seeing how US Government agencies use the NIST Cybersecurity Framework would be incredibly valuable for organizations currently using, or considering using, the Framework.

14. Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.

To reiterate, as NIST integrates more information into the Framework, it is important to ensure the Framework does not grow past the point of diminishing marginal returns. Too often government policies take a "more is better" approach to improving cybersecurity, and an important driver of the value the Cybersecurity Framework creates is in removing information that is less impactful so that organizations can focus on actions that are more impactful. That being said, explaining where and how cybersecurity supply chain risk management (C-SCRM) fits in to the five functions, and how its consideration might impact an organization's implementation tier would improve the Framework. NIST should particularly consider the subcategory ID.BE: The organization's role in the supply chain is identified and communicated. Further, identifying priorities within NIST's current C-SCRM guidance, would add value to the Framework.

# # # #

BSA appreciates the opportunity to provide the above comments and looks forward to working with NIST to improve the NIST Cybersecurity Framework.



Henry Young
Director, Policy

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org